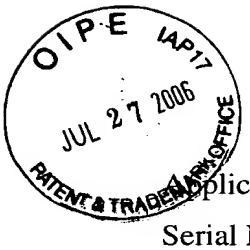

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Before the Board of Patent Appeals and Interferences

Applicant	:	Eskicioglu et al.
Serial No.	:	09/581,064
Filed	:	October 7, 2002
For	:	CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS
Examiner	:	Klimach, Paula W.
Art Unit	:	2135

07/27/2006 CHEGA1 00000033 070832 09581064
01 FC:1402 500.00 DA

APPEAL BRIEF

May It Please The Honorable Board:

This is Appellants' Brief on Appeal from the final rejection of Claims 1 – 7, a Notice of Appeal having been filed on November 2, 2005, the instant Brief originally due January 4, 2006. A Petition to Revive under 37 CFR 1.137(b) is attached herewith. Please charge the fee for the Petition and the $500.00 fee for filing this Brief to Deposit Account No. 07-0832. Appellants waive an Oral Hearing for this appeal.

Please charge any additional fee or credit overpayment to the above-indicated Deposit Account. Enclosed is a single copy of the Brief.

I. REAL PARTY IN INTEREST

The real party in interest of Application Serial No. 09/798,739 is the Assignee of record:

THOMSON (formerly THOMSON MULTIMEDIA)
46 QUAI ALPHONSE LE GALLO
F-92100 BOULOGNE BILLANCOURT, FRANCE

II. RELATED APPEALS AND INTERFERENCES

Application Serial Nos. 09/961,835 (Atty. Dkt. PU000134) and 09/961,901 (Atty. Dkt. PU010197) have appeals pending. There are currently, and have been, no other related Appeals or Interferences regarding the subject application known to the undersigned attorney.

****

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in a postage paid envelope addressed to: Mail Stop: Appeal Briefs - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

Signature Lori M. Kleuri Date: July 25, 2006

III. STATUS OF THE CLAIMS

Claims 1-7 are rejected. The rejections of Claims 1-4 are appealed. Claims 5-7 have been cancelled in the amendment filed contemporaneously herewith, a copy of which is attached hereto as Appendix I.

IV. STATUS OF AMENDMENTS

All prior amendments were entered. The claims included in Appendix I reflect each of the prior amendments, and the amendment filed contemporaneously herewith, a copy of which is attached hereto as Appendix IV.

V. SUMMARY OF CLAIMED SUBJECT MATTER

This summary sets forth exemplary reference characters and pages and line numbers in the specification where an embodiment of each separately argued claim is illustrated or described. The identification of reference characters and pages and line numbers does not constitute a representation that any claim element is limited to the embodiment illustrated at the reference character or described in the referenced portion of the specification.

Independent Claim 1 recites a method for managing access to a signal representative of an event of a service provider. *(See, e.g., specification, page 2, ll. 10-31).* The method includes, (a) receiving said signal in a smart card, said signal being scrambled using a scrambling key. *(See, e.g., specification, page 2, ll. 10-31; see also, specification page 6, ll. 5-6).* The method further includes, (b) receiving, in said smart card, data representative of a first seed value; *(see, e.g., specification, page 2, ll. 23-31; see also, specification, page 6, ll. 6-7)* and (c) generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, whereby secret sharing is implemented. *(See, e.g., specification, page 2, ll. 23-31; see also, specification, page 6, ll. 14-20; see also, Fig. 3a).* Claim 1 recites that the second seed value is permanently stored in said smart card. *(See, e.g., specification, page 2, ll. 23-31; see also, specification, page 5, ll. 32-33; see also, specification, page 6, ll. 5-12; see also, page 7, ll. 8-10).* Finally, the method of Claim 1 includes, (d) descrambling, in said smart card, said signal using said generated scrambling key to provide a descrambled signal. *(See, e.g., specification, page 2, ll. 10-21; see also, specification, page 6, ll. 9-11).*

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner has finally rejected Claims 1-4 as being unpatentable under 35 USC 103(a) over United States Patent No. 6,035,037 (hereinafter referred to as Chaney) in view of the article "How to Share a Secret" appearing in Communications of the ACM, Volume 22, pages 612-613 (1979) by Adi Shamir (hereinafter referred to as Shamir).

VII. ARGUMENT

The recited method of Claim 1 is patentable over Chaney in view of Shamir, at least by virtue that: (1) Chaney and Shamir fail, in any combination, to teach or suggest each of the recited limitations of Claim 1; and (2) a proper motivation for modifying the teachings of Chaney and/or Shamir asserted by the Examiner in an attempt to reach the invention of Claim 1 does not exist, absent impermissible hindsight based on Appellant's disclosure.

A. Standard For Unpatentability Pursuant to 35 U.S.C. 103(a)

To establish a *prima facie* case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).* To establish a prima facie case of obviousness, there must also be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P. 706.02(j).* Further yet, the teaching or suggestion to make the claimed combination must not be based on the applicant's own disclosure. *In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).*

B. Claim 1 Recites a Method that Generates a Scrambling Key in a Smart Card Using: (1) a Received First Seed Value; (2) a Second Seed Value Permanently Stored in the Smart Card; (3) in a Predetermined Function.

The subject invention concerns a system for providing conditional access to received scrambled signals, such as audio/visual (A/V) signals received from broadcast television networks, cable television networks, digital satellite systems and Internet service providers. *See, e.g., specification, page 1, ll. 8-11.* The method of Claim 1 calls for a smart card to generate a key for descrambling the received signals using a first seed value received from the service provider of the signal to be descrambled, in combination with a second seed value

permanently stored in the smart card, in a predetermined function. *See, e.g., specification, page 2, ll. 23-31.* Such a method advantageously uses reduced computational requirements, as compared to conventional Data Encryption Standard (DES) key recovery. *See, e.g., specification, page 5, ll. 23-24.*

Claim 1 is drawn to a method for managing access to a signal representative of an event of a service provider. By way of example, the signal (*e.g.*, an event or program) may take the form of audio/visual data, such as a movie, weekly show, or a documentary. *See, e.g., specification, page 2, ll. 10-12.* It is desirable to manage access to the signal, and hence access to the underlying content, e.g., a movie, weekly show, or a documentary – in other words provide conditional access. *See, e.g., specification, page 2, ll. 23-25; see also, specification, page 1, ll. 19-29.*

To provide conditional access, the method of Claim 1 recites in part, "(b) receiving, in said smart card, data representative of a first seed value". As is explained in the specification, a service provider transmits both a scrambled signal and a first seed value, which are coupled into a smart-card. *See, e.g., specification, page 5, l. 35 –page 6, l. 6.*

The method of Claim 1 also recites, "(c) generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function." As explained in the specification, a symmetric key is recovered by constructing a polynomial using the first seed value that was received from the service provider and a second seed value. *See, e.g., specification, page 6, ll. 14-15.* In the example discussed in the specification, one of the seeds is (x0, y0) and the other of the seeds is (x1, y1). *See, e.g., specification, page 6, ll. 16-17.* The specification goes on to explain that in such a case, the symmetric key is generated by computing the value of $[\{(y1-y0)/(x1-x0)\}(x-x0)] + y0$ at $x=0$. *See, specification, page 6, ll. 17-19.* This is shown in Fig. 3a of the subject application. *See, specification, page 6, ll. 19-20.*

The method of Claim 1 also recites that, "said second seed value [is] permanently stored in said smart card." As is discussed in the specification, a seed value (or data point) is stored in the smart card. *See, e.g., page 5, ll. 32-34.* The approach of using a seed value received from a service provider in combination with a seed value stored in a smart card, to calculate a key for descrambling a scrambled signal in the smart card, permits more than one service provider to share the stored seed value, and choose its own seed value to transmit to the smart card – and hence specify its own key for its own signals. *See, e.g., specification, page 6, ll. 21-26.* Such a methodology minimizes the amount of information that needs to be

stored in a smart card to permit access to multiple service providers. *See, e.g., specification, page 6, l. 35 – page 7, l. 2.*

The method of Claim 1 also recites, descrambling, in said smart card, a scrambled signal also received in the smart card, using the key generated in the smart card in steps (a) and (d). This is discussed in the subject application wherein a scrambled A/V signal is coupled into the smart card for processing, and the smart card reconstructed key is used by the smart card to descramble the scrambled A/V signal. *See, e.g., specification, page 6, ll. 5-12.*

Thus, Claim 1 clearly calls for a smart card to: (1) generate a scrambling key using a first seed value received by the smart card and a second seed value permanently stored in the smart card; and (2) descramble a signal received in the smart card using the generated scrambling key. Accordingly, in order to render Claim 1 unpatentable under 35 U.S.C. 103(a), Chaney and Shamir must teach each of these limitations. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).*

C. No Combination of Chaney and Shamir Teaches or Suggests Generating a Scrambling Key in a Smart Card Using a First Seed Value Received by The Smart Card and a Second Seed Value Permanently Stored in the Smart Card

Chaney teaches a system that uses first and second smart cards to produce an image that includes multiple image portions, such as picture in picture (PIP) or picture outside picture (POP). *See, e.g., col. 3, ll. 3-7, 17-21.* The Final Office action essentially argues Chaney teaches steps (a) and (d) of Claim 1, namely: receiving a scrambled signal in the smart card, that a scrambling key is stored in the smart card, and descrambling the scrambled signal in the smartcard using the key. *See, 7/12/2005 Office action, page 4, ll. 19-24.* The Final Office action admits that Chaney fails to teach generating a key in the smart card based on a first seed value received in the smart card and a second seed value being permanently stored in the smart card – *i.e.*, the limitations recited in Claim 1 steps (b) and (c). *7/12/2005 Office action, page 5, ll. 1-5.*

The appealed rejections rely on Shamir to remedy this admitted deficiency of Chaney. The appealed rejections argue Shamir discloses secret sharing, wherein the key is divided into pieces, each party possesses one of the pieces, and to obtain the key a threshold number of the keys must be combined in a predetermined fashion. *7/12/2005 Office action, page 5, ll. 6-9.* The appealed rejections then conclude it would thus have been obvious to divide a key into

pieces as in Shamir and express a key based on the received key, from the other parties, and combine it with the key stored in the smart card of Chaney. *7/12/2005 Office action, page 5, ll. 10-12.* According to the Examiner, one of ordinary skill in the art would have been motivated to do this because dividing the key into pieces and distributing the key provides a robust key management system. *7/12/2005 Office action, page 5, ll. 12-14.* Appellant traverses these assertions.

First, Appellant respectfully submits that the Examiner misapprehends and misapplies the actual teachings of Shamir. Shamir asserts that its technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces. *See, Abstract.* Within this context, Shamir discloses its threshold scheme is ideally suited for where there are a number of mutually suspicious individuals with conflicting interests that must cooperate. *See, e.g., col. 2, ll. 47-49.* Shamir provides a working example of its threshold scheme in the nature of a company that digitally signs its checks, and requires three executive signatures per check. *See, col. 2, ll. 30-36.* In such a case, each of the executives is considered to be mutually suspicious, such that three of them must cooperate to actually sign a check. *See again, col. 2, ll. 30-36.* In this example, Shamir teaches that a (3, n) threshold scheme may be used. *See, col. 2, ll. 36-37.* In such a (3, n) scheme, each of the executives is provided with a magnetic card, where each magnetic card contains a single key piece, or share (D_i). *See, col. 2, ll. 38-39.* The company's signature generating device accepts any three of the key pieces (D_i) to generate (and later destroy) a temporary copy of the actual company signature key D. *See, col. 2, ll. 39-42.*

Shamir further discloses that its signature generating device, *i.e.*, the device that receives and uses the "executive-held" key pieces (D_i) to generate actual key D, does not contain any secret information. *See, col. 2, ll. 42-44 (The device does not contain any secret information and thus it need not be protected against inspection).* Thus, Shamir does not teach or suggest generating a scrambling key in a device using a piece (D_i) received in the device and another piece (D_j) permanently stored in the device. Accordingly, like Chaney, Shamir fails to teach generating a scrambling key in a smart card using a first seed value received by the smart card and a second seed value permanently stored in the smart card, as is recited by steps (b) and (c) of Claim 1.

On Page 3, ll. 7-11 of the Final Office action, the Examiner states:

> Shamir discloses the executive saving the key [share] on a small magnetic card, and therefore storing secret key shares in a

> signature. The reference teaches against storing the complete computed key that is computed from all the shares of the other members. The reference says that all the pieces are required to forge a signature therefore there is no need to protect the device. However, the expression "it need not be protected," does not rule out protecting the portion of the key and therefore create greater security.

Appellant notes that Shamir expressly recites, "[t]he [piece D_i using] device does not contain any secret information and thus it need not be protected against inspection." *Col. 2, ll. 42-44*. Each key piece, or share, D_i is clearly secret – otherwise, if the key pieces were public, anyone could merely collect three of them and forge the company's signature. Whether or not one could optionally secure the device itself does not change Shamir's clear teaching that the device does not contain any secret information.

Further, in the only example discussed at length, Shamir discloses that where three executives must sign a check, a (3, n) threshold scheme may be implemented – that is, at least 3 of the n executives must provide their key pieces (D_i) to the check signing device. Shamir further discloses that, "[a]n unfaithful executive must have at least two other accomplices in order to forge the company's signature scheme." *Col. 2, ll. 44-46*. These teachings are entirely inconsistent with the position asserted by the Examiner in the Final Office action and in the Advisory action (*See, 9/26/2005 Advisory Action continuation of 11*) that Shamir teaches or suggests permanently storing one of the key pieces D_i in the key D generating device itself – otherwise, only two executives, or one accomplice, would be needed to sign or forge a check, as one of the necessary three key pieces D_i in the (3, n) scheme would already be present in the key generating device.

Further yet, it is clear that the magnetic cards disclosed in Shamir, which each store a single key piece or key share D_i, cannot be equated to the recited smart card of Claim 1 – which receives a first seed value in addition to permanently storing a second seed value and which itself is recited to generate the scrambling key and descrambles the content. In contrast, Shamir expressly teaches a separate key generating device (*e.g.*, check signing device) receives and processes the pieces D_i.

Accordingly, as neither Shamir nor Chaney teach or suggest:

> (b) receiving, in said smart card, data representative of a first seed value; [and]
>
> (c) generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, whereby secret sharing is

implemented, said second seed value being permanently stored in said smart card;

as is recited by Claim 1, their combination necessarily fails to teach or suggest these features and limitations as well.

D. No Proper Motivation Exists For Modifying The Combined Teachings Of Chaney And Shamir To Reach The Invention Of Claim 1

The Final Office action argues "it would thus have been obvious to divide a key into pieces and express a key based upon the received key and combine it with the key stored in the smart card of Chaney". *7/12/2005 Office action, page 5, ll. 10-12.* Appellant traverses this assertion.

As acknowledged in the Final Office action, Chaney fails to teach generating a key from two seed values in a predetermined function at all. Moreover, and as discussed above, Shamir expressly teaches against storing any key pieces, or shares, in the key generating device.

Each prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984).* And, a *prima facie* case of obviousness can be rebutted when a person of ordinary skill, upon reading a cited reference, would be led in a direction divergent from the path that was taken by the applicant. *In re Haruna, 249 F.3d 1327, 58USPQ2d 1517.*

Not only does Shamir lead the skilled artisan down a different path than that recited by Claim 1, but the teachings of Shamir actually contradict the method of Claim 1 that recites permanently storing the second seed value in the same device that receives the first seed value and uses the seed values in a predetermined function. That is, Shamir teaches against storing any key share in a device that receives and uses other shares. In Shamir's (3,n) scheme, three of the executives must cooperate to actually sign a check. *See again, col. 2, ll. 30-36.* The company's signature generating machine accepts any three of the key pieces (D_i) to generate (and later destroy) a temporary copy of the actual company signature key D. *See, col. 2, ll. 39-42.*

Again, whether or not one may decide to secure the signature generating device of Shamir, Shamir teaches that it need not be protected because it does not contain any secret information. The present rejection necessarily discounts Shamir's prohibition from storing

secret information in the share receiving and utilizing device to modify the Chaney system to incorporate its share methodology, yet also store at least two key shares in a key generating smart card. This is improper. Shamir must properly be considered in its entirety, including its teachings against storing secret information in the key constructing device.

Accordingly, a proper motivation does not exist for modifying the Chaney reference to incorporate the Shamir share methodology, while also storing key shares in a share receiving and key constructing smart card in direct contradiction to Shamir's prohibition thereof, absent impermissible hindsight gleaned from Appellant's own disclosure.

VIII. CONCLUSION

Reversal of the 35 USC 103(a) rejection of Claim 1 is therefore requested, at least by reason that: (1) Chaney and Shamir fail, in any combination, to teach each of the recited limitations of Claim 1 – namely at least recited steps (b) and (c) thereof; and (2) a proper motivation for combining the Chaney and Shamir references to reach the recited method of Claim 1 – namely generating a scrambling key in a smart card using a first seed value received by the smart card and a second seed value permanently stored in the smart card is lacking, at least by reason that Shamir teaches against such an implementation.

Appellant also respectfully requests reversal of the 35 U.S.C. 103(a) rejections of Claims 2-4, at least by virtue of these claims' ultimate dependence from patentably distinct base Claim 1.

Respectfully submitted,

By: Paul P Kiel 7/25/06

Paul Kiel, Attorney
Registration No. 40,677
(609) 734-6815

Patent Operations
Thomson Licensing
P.O. Box 5312
Princeton, NJ 08543-5312

APPENDIX I - APPEALED CLAIMS

1. (Previously Presented) A method for managing access to a signal representative of an event of a service provider, said method comprising:

(a) receiving said signal in a smart card, said signal being scrambled using a scrambling key;

(b) receiving, in said smart card, data representative of a first seed value;

(c) generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card; and

(d) descrambling, in said smart card, said signal using said generated scrambling key to provide a descrambled signal.

2. (Previously Presented) The method of Claim 1 wherein said first and second seed values are points on a Euclidean plane.

3. (Previously Presented) The method of Claim 2 wherein the step of generating said scrambling key comprises calculating the Y-intercept of a line formed on said Euclidean plane by said first and second seed values.

4. (Previously Presented) The method of Claim 3 wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMICA card standards.

APPENDIX II - TABLE OF CASES

In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)

In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984)

In re Haruna, 249 F.3d 1327, 58USPQ2d 1517

APPENDIX III - LIST OF REFERENCES

PATENTS

U.S. Pat. No.	Issued Date	102(e) Date	Inventors
6,035,037	03/07/2000	01/30/1997	Chaney

NON- PATENT REFERENCES

"How to Share a Secret" appearing in Communications of the ACM, Volume 22, pages 612-613 (1979) by Adi Shamir

TABLE OF CONTENTS